Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/SG05/000084

International filing date: 17 March 2005 (17.03.2005)

Document type: Certified copy of priority document

Document details:
Country/Office: AU
Number: 2004901393
Filing date: 17 March 2004 (17.03.2004)

Date of receipt at the International Bureau: 15 April 2005 (15.04.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

PCT/SG 2005/000084

Australian Government

Patent Office
Canberra

I, JANENE PEISKER, TEAM LEADER EXAMINATION SUPPORT AND SALES hereby certify that annexed is a true copy of the Provisional specification in connection with Application No. 2004901393 for a patent by DIGISAFE PTE LTD as filed on 17 March 2004.

COMMONWEALTH OF AUSTRALIA
AUSTRALIA
PATENT OFFICE

WITNESS my hand this
Twenty-fourth day of March 2005

JANENE PEISKER
TEAM LEADER EXAMINATION
SUPPORT AND SALES

AUSTRALIA

Patents Act 1990

PROVISIONAL SPECIFICATION

Applicant:

DIGISAFE PTE LTD

Invention Title:

METHOD AND APPARATUS FOR PROTECTING DATA STORED IN A COMPUTING DEVICE

The invention is described in the following statement:

METHOD AND DEVICE FOR PROTECTING DATA STORED IN A COMPUTING DEVICE

FIELD OF THE INVENTION

The present invention relates to a method and device for protecting data stored in a computing device, of particular but by no means exclusive application in protecting data stored in a portable computing device.

BACKGROUND TO INVENTION

Computers and other computing devices are used to store important data that can be easily compromised when an unauthorized user illegally accesses the device, or when the device is stolen.

In the case of portable computers, such as personal digital assistants, laptop computers and notebook computers, the risk is particularly high owing to the greater ease with which such devices can be misplaced or stolen. According to Kensington Technology Group Notebook Security Survey 2001 and 2003 CSI/FBI Computer Crime & Security Survey, a typical medium-sized company loses about 11 notebooks annually, with an average financial loss of US$64,000 per notebook.

Existing software exists in which the hard disk of a notebook is protected by encryption. These software solutions have inherent problems, which include operating system dependencies, a need for device drivers, and a need for patches when the device is upgraded, and the like. Most software solutions also leave the operating system unencrypted.

Hardware solutions exist in which an additional interface is added between the hard disk and the device's IDE/ATA (Integrated Drive Electronics/AT Attachment) bus. Although such interfaces do not have the problems associated with the software solutions described above, these hardware solutions cannot be easily implemented on portable computing devices such as notebook computers because additional interface hardware cannot be accommodated in the space normally occupied by, in a notebook computer, a hard disk. In addition, these hardware solutions often require an additional interface into which a hardware key is inserted in order to authenticate the user to the hardware encryptor before activating the hardware encryption/decryption device. This interface is necessary because the hardware solution has no way of interfacing to other authentication devices, such as keyboards. This hardware interface cannot, therefore, be implemented on the portable computing device without customizing the device.

SUMMARY OF THE INVENTION

It is an object of the present invention, therefore, to provide a method and device for protecting data stored in a computing device, such as a notebook computer.

The present invention provides a device for protecting data, comprising:

an interface for connection to a computing device;

a data storage;

an encryptor located in-line between said interface and said data storage;

wherein said encryptor is operable to encrypt on the fly data written through said interface to said data storage and to decrypt on the fly data read through said interface from said data storage.

Thus, the data stored in the data storage is encrypted, but the user need not be aware of the encryption or decryption processes.

The computing device could be any such device, but the invention will provide particular benefit with portable computing devices that – as discussed above – are most vulnerable to unauthorized data access.

The present invention also provides a method of protecting data, comprising:

locating an encryptor in-line between a data storage and an interface to a computing device; and

encrypting on the fly data written through said interface to said data storage and decrypting on the fly data read through said interface from said data storage.

BRIEF DESCRIPTION OF THE DRAWINGS

In order that the invention may be more clearly ascertained, preferred embodiments will now be described, by way of example, with reference to the accompanying drawings, in which:

Figure 1 is a schematic view of a data protection device according to an embodiment of the present invention, with a portable computing device with which the device is to be used;

Figure 2 is a photograph of the data protection device of figure 1; and

Figure 3 is a schematic view of the functional components of the data protection device of figure 1.

DETAILED DESCRIPTION OF THE INVENTION

A data protection device according to an embodiment of the present invention is shown generally at 10 in figure 1, together with a portable computing device in the form of a notebook computer 12 with which the device 10 is to be used. The notebook computer 12 includes an integrated CPU/keyboard case 14 and an LCD display 16. In use, the device 10 is located within the CPU/keyboard case 14 and so in not visible.

The device 10 has the same form factor and hardware interface as the standard data storage device (viz. a hard disk) that would normally be provided in the notebook computer 12; device 10 thus replaces that usual storage device, and is designed to be mounted within a notebook computer like any ordinary 2.5" hard disk for notebooks.

The device 10, however, contains a hardware encryption module together with its own storage medium as is described below. The device 10 thus requires neither an additional hardware interface, nor an additional interface for a hardware key to be inserted.

Figure 2 is a photograph of the data protection device of figure 1, while figure 3 is a block diagram of the functional components of device 10. These components include an interface 18 of the same type as the hardware interface for the standard storage medium otherwise used by notebook computer 12.

Device 10 also includes an encrypted storage medium 20 (in this embodiment, a hard disk) and an in-line encryptor 22 for the encrypted storage medium 20. The in-line encryptor 22 is exposed to the hardware interface 18, and performs encryption and decryption on the fly when data is written or read through the interface 18.

Device 10 further includes multiple storage system 24, which is exposed to the hardware interface 18, and contains bootable programs 26 for the notebook computer 12. These bootable programs 26 are used for, but are not limited to, the following functions:
1) Authentication of users upon powering on the notebook computer 12;
2) Simulation of a normal booting process so that users need not realize that there is protected data inside the device 10. For this notebook hard disk implementation,

storage system 24 contains not only bootable programs 26 but also the boot record 28 necessary to load the bootable program 26.

Storage system 24 may alternatively be implemented using microprocessors or logic that interface with non-volatile memory or a storage medium.

The device 10 further includes a control system 30, which is the overall control system of the device 10. The bootable programs 26 can communicate with control system 30 through interface 18, via bridge 32 implemented within storage system 24. The control system 30 controls the in-line encryptor 22 via a further bridge 34.

The specifications of the components of the device 10 are as follows:

Storage Capacity & Speed	• 20 GB • 66MB/s Ultra DMA Transfer Rate
Operating System	• Operating system independent • Tested with: Windows 98 (TM), Windows 2000 (TM), Windows XP (TM) and Linux (TM)
Interface & Mechanical	• Standard 2.5" HDD. Complies to SFF-8200, SFF-8201, SFF-8212 • Size: 100(L)×70(W)×9.5(H) mm
Encryption Algorithm	• 3DES ("Triple Data Encryption Standard"); key lengths from 40 to 192 bits
Authentication Mechanisms	• Pre-boot authentication • Password or USB cryptographic token
Certifications and Standards	• Designed to meet FIPS140-2 Level 2 • CE, FCC

When the device 10 is in use, the bootable programs 26 can also access devices connected to the notebook computer 12. These devices include authentication devices or devices for inputting authentication data, including a keyboard, a smart card, a USB token 36 or a biometric device.

The operational flow of the device 10 is as follows:

(1) Upon powering on the notebook 12 and hence device 10, the control system 30 exposes one unit of the storage system 24 and hides the in-line encryptor 22.

(2) One of bootable programs 26 is loaded into the notebook computer 12, in the normal power-on process for the notebook computer 12. In this notebook hard disk embodiment, boot record 28 is loaded by the notebook computer 12, which loads this bootable program.

(3) This bootable program executes in notebook computer 12. It could execute to emulate a normal booting process as a decoy, or it could authenticate the user to authorize him to access encrypted storage 20 via in-line encryptor 22. In the latter case, the bootable program authenticates the user by requesting that the user authenticate him- or herself using the relevant authentication device provided in or with the notebook computer 12. This could be implemented, for example, by:

(a) requesting that the user type in his or her password using a keyboard;
(b) requesting that the user type in his or her password and insert a smartcard or USB token; or
(c) requesting that the user present his biometric data, such as a fingerprint or iris scan.

(4) The bootable program communicates with the control system 30.

(5) If the user is authorized, the bootable program restarts the notebook computer 12, while control system 30 activates in-line encryptor 22 and exposes its interface by means of bridge 34 to interface 18.

(6) When the notebook computer 12 boots a second time, inline encryptor 22 decrypts the operating system within storage system 20, and the device 10 can be used as normal from this point onwards.

Thus, device 10 operates independently of the operating system installed on the storage medium it is protecting, and it can support multiple methods of authentication including password, smart card, USB token, etc. The device 10 can interface to an external authentication device, such as a smart card, USB token, etc., using existing interface(s) available on the host computer 12, and it can support one or more bootable programs 26 in addition to the storage medium 20 it is protecting.

As the device 10 is designed to a drop-in replacement for a notebook hard disk, it provides a convenient means for providing high data security in a notebook computer. This is particularly so when used with a USB security token 30 36.

The device 10 allows the encryption of every byte and every sector of data that is written into the hard disk 20. By encrypting every byte and sector, the device 10 is operating system independent, does not require any software drivers and thus users will not experience problems associated with software incompatibilities and patches. The device 10 encrypts all temporary files and areas that would normally be left vulnerable or "clear" by software file encryption products. Once a user is authenticated upon powering-on, encryption and decryption occurs transparently on-the-fly in the hardware without any degradation in notebook or disk performance. Users can use their notebooks normally, but with their data fully protected should their notebooks be stolen or lost.

Modifications within the scope of the invention may be readily effected by those skilled in the art. It is to be understood, therefore, that this invention is not limited to the particular embodiments described by way of example hereinabove.

In the preceding description of the invention, except where the context requires otherwise owing to express language or necessary implication, the word "comprise" or variations such as "comprises" or "comprising" is used in an inclusive sense, i.e. to specify the presence of the stated features but not to preclude the presence or addition of further features in various embodiments of the invention.

Further, any reference herein to prior art is not intended to imply that such prior art forms or formed a part of the common general knowledge.

Dated this 17th day of March 2004
DIGISAFE PTE LTD
By their Patent Attorneys
GRIFFITH HACK
Fellows Institute of Patent and
Trade Mark Attorneys of Australia

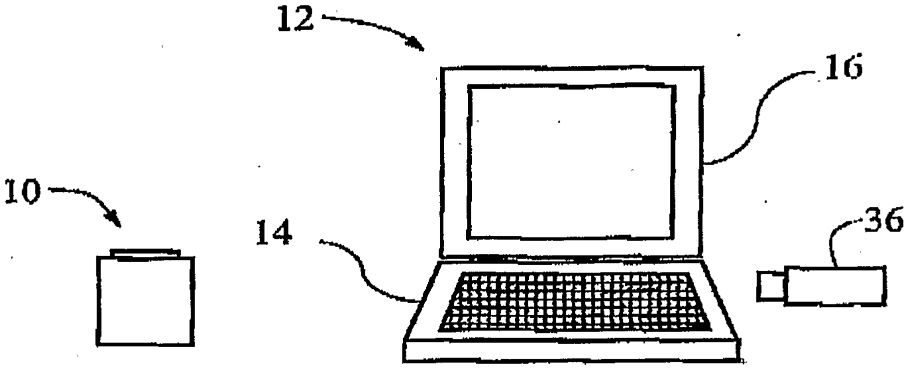

Figure 1

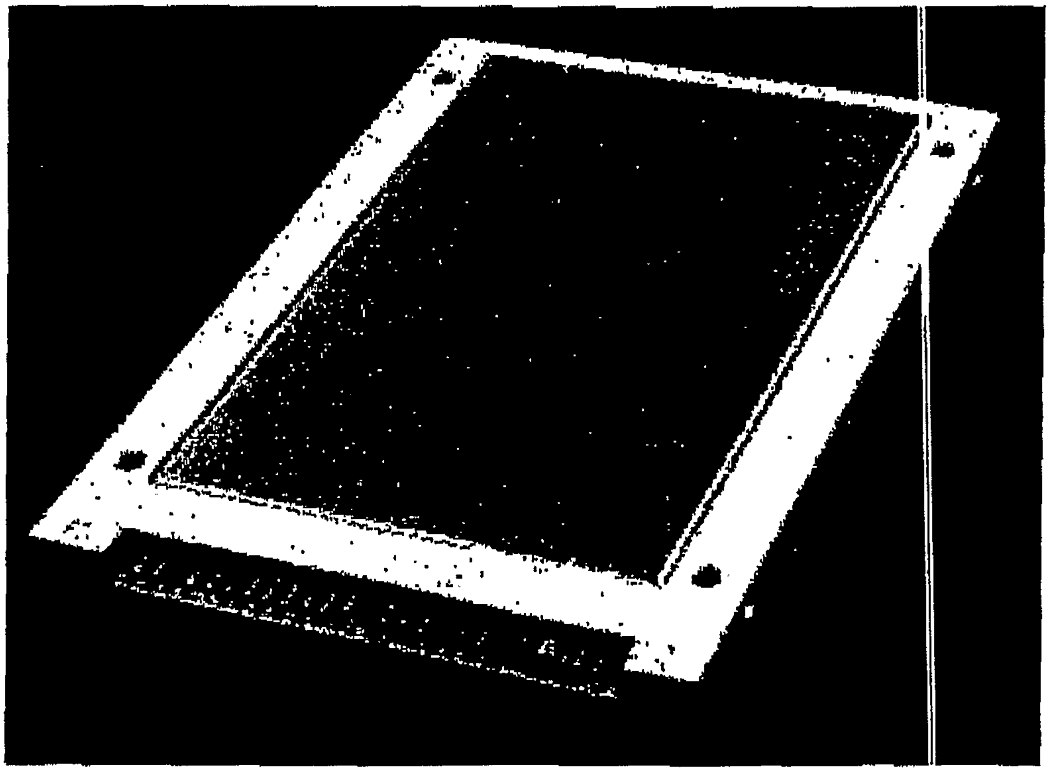

Figure 2

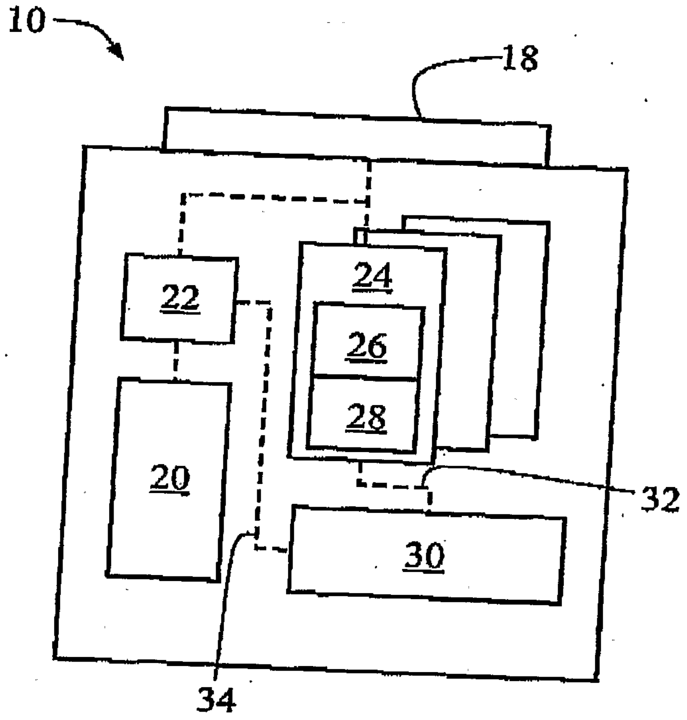

Figure 3